



Converged Messaging Security Threats

Questnet

July 2007 - Cairns



Dean Bell
dean@borderware.com

Company Introduction

- Founded in 1994 from Border Network Technologies
- 10,000 Customers in 65 countries
- 500 Channel Partners
- Headquartered in Toronto, Canada
- Offices in Dallas Texas, San Jose California, Toronto Canada, London UK, Frankfurt Germany, Stockholm Sweden, Australia and Dubai.
- Alliance Partners: Cisco, F5, FaceTime, Kaspersky Labs, McAfee, Marconi, PGP, PostX, RIM, RSA, Sun, SurfControl, Symantec, Ubiquity
- Innovation: 1st Application Proxy Firewall, 1st SMTP Firewall, 1st SIP Firewall
- Wide range of products
 - Steel Gate Application Proxy Firewall/VPN Appliance
 - MXtreme™ Mail Firewall and Anti Spam Appliance
 - SIPassure SIP based firewall, SIP Gateway and SIP Server
 - BorderWare Security Platform, Mail, IM, HTTP/FTP, VoIP
- Unbeaten Security Certification Track record – 13 years!
 - First Ever Firewall Common Criteria EAL4/EAL4+ certification
 - Only Firewall to have passed EAL5 Vulnerability Analysis
 - Australian Government DSD approval



July 2007

© Copyright 2007 BorderWare Technologies Inc. All Rights Reserved.

2

BorderWare World Class Customers

Health Care	Technology	Retail & Services	Food & Beverage	Transportation

July 2007 © Copyright 2007 BorderWare Technologies Inc. All Rights Reserved. 3

BorderWare World Class Customers

Government	Telecom & ISP	Media	Automotive	Finance & Insurance

July 2007 © Copyright 2007 BorderWare Technologies Inc. All Rights Reserved. 4

Reference customers - Australia

- Schiavello Commercial Interiors
- The Muir Electrical Company
- Austereo Pty Ltd.
- Laminex Industries
- Centari Systems
- East Gippsland Shire Council
- Catholic Development Fund
- Esprit Australia
- City of Boroondara
- Sussan Corporation Australia
- Ecowise Environmental Pty Ltd
- Western Water Limited
- Spalding Australia
- HLB Mann Judd
- Yakult Australia
- Fuchs Lubricants Pty Ltd
- Mushroom Music
- Australian Sports Commission
- Visa Australia
- North Shore Coaching Centre
- 7-Eleven Stores Pty Ltd.
- Breville Pty Ltd.
- Sydney Markets Limited
- Moore Connections Pty. Limited
- EIG - Ansvar Limited
- William Adams Pty Ltd
- Eurovox Pty Ltd
- Holmesglen Institute of TAFE
- Telstra Super Pty Ltd
- Equity Trustees Limited
- Queensland Government Department of Employment & Training
- Northern Melbourne Institute of TAFE
- Metropolitan Ambulance Service
- Department of Environment
- Attorney-General's Dept
- Mortgage Data Solutions
- Australian Industrial Registry
- VicSuper Pty Ltd
- Bob Jane T-Marts Pty Ltd
- Airborne Research Australia
- AusAID
- HGC Administrative Services
- Sorrento Sailing Boat Club
- Department of Defence
- TechExpress IT Solutions
- GAPBuster Systems Asia Pacific Ltd.
- Absolute Data Group
- Red Bull Australia Pty Ltd
- Chanel (Australia) Pty Ltd
- The National Office for the Information Economy
- Australian Film Commission
- Dorf Clark Industries Limited
- The Australian Inst of Building
- Peter MacCallum Cancer Inst
- Pacific National (ACT) Ltd.
- Australian Motoring Services



July 2007

© Copyright 2007 BorderWare Technologies Inc. All Rights Reserved.

5

Reference customers – Australia cont'd

- Ozemail
- City of Perth
- AAP Communications
- Macquarie Universit
- The Siemon Company
- MacMillan Distribution
- Animal Logic
- Department of Environmental Protection
- Gippsland Water
- Pulsat Communications
- Ozemail
- Bendigo Bank
- William Angliss TAFE
- Tower Life Ltd.
- Office of Indigenous Policy Coordination
- CBT Systems Australia
- Fisheries Dept of WA
- Queensland Transport
- Dynamic Solutions
- State Supply Commission
- Sprucer & Ferguson
- BMW Australia
- Acer Computer
- Aboriginal & Torres Strait Islander Commission
- Travelex Australia Pty Ltd
- Adept Business Systems
- Macquarie University
- APRA Ltd.
- Quik Trak Technologies
- Rudd Watts & Stone
- Austrust - Tower Financial Services
- Local Government and Shires Association
- Sydney South West Area Health Service
- Brimbank City Council
- Australian Trade Commission
- Ministry of Justice
- South Australia Auditor-General's Department
- "Department of Defense Emergency Management, DEFMIS "
- Sloane, Duff & Associates
- Community News Group
- Flexirent Capital Pty Ltd
- Professionals in Computer Knowledge
- Copyright Agency
- Dyno Industries
- Global Doctor Services
- CARE Australia
- Australian Fisheries Auth
- Hatch Associates Pty. Ltd.
- Hamilton Brokers Pty Ltd.
- Pinnacle Software
- Australian Pesticides & Veterinary Medicines
- High Court of Australia
- Allied Telesyn International
- Royal College of Pathologists of Australasia
- City Of Melbourne
- Phoenix Corporation
- Sci-Qual International
- Leigh-Mardon
- Australian Pacific Touring

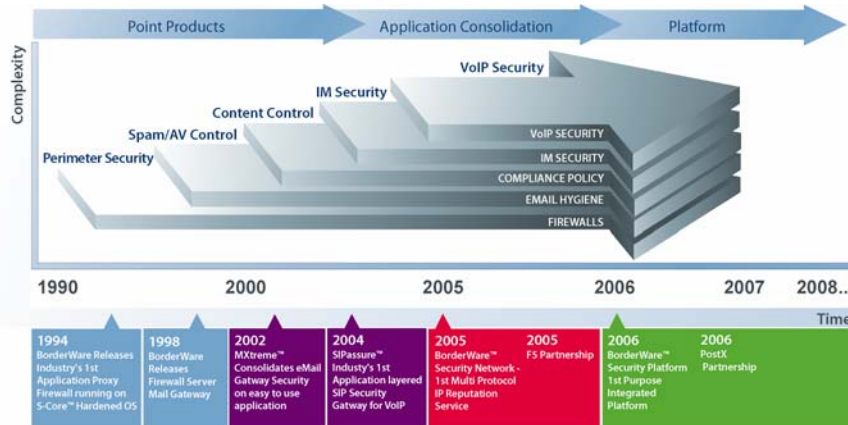


July 2007

© Copyright 2007 BorderWare Technologies Inc. All Rights Reserved.

6

13 years technology roadmap – thought leadership



BorderWare™

July 2007

© Copyright 2007 BorderWare Technologies Inc. All Rights Reserved.

7

Agenda

- Threats – case study
 - Mail threats
 - HTTP/FTP
 - IM
 - VoIP
- Security Threats
- Business Risks
- Addressing the Challenges

BorderWare™

July 2007

© Copyright 2007 BorderWare Technologies Inc. All Rights Reserved.

8

The Threats Are Real & Current – 2005/2006

- MasterCard - 40 million customer records leaked in June 2005 - case study
- Virgin Money - A flood of phishing emails sent out targeting Virgin Money credit card customers in September 2005
- Chevron - \$2M lawsuit from an employee "joke" email with alleged sexist content
- Health Care Company - Patient records divulged
- Pharmaceutical Company - Intellectual property leaked to a competitor
- Law Firm – Confidential email communications compromised
- VoIP spam, vishing, DHA - infancy



BorderWare

July 2007

© Copyright 2007 BorderWare Technologies Inc. All Rights Reserved.

9

Case study

External impact of inadequate security - MasterCard

In June 2005, 40 million MasterCard customer records were accidentally leaked

- The culprit was an outsourcing partner, CardSystem Solutions, a payment processor with only 100 employees that was the victim of a hacking attack
- Huge impact on MasterCard, whose customers saw them as at fault
- Huge impact on CardSystem Solutions, who lost all other customers Visa and American Express, went out of business and are now being sued for breach of security and SLA

Visa commented: *"after an internal and forensics review of its processing practices demonstrated that -- in violation of Visa's SLA -- it did not have the appropriate controls in place to protect cardholder information."*

Legal Liability!!!

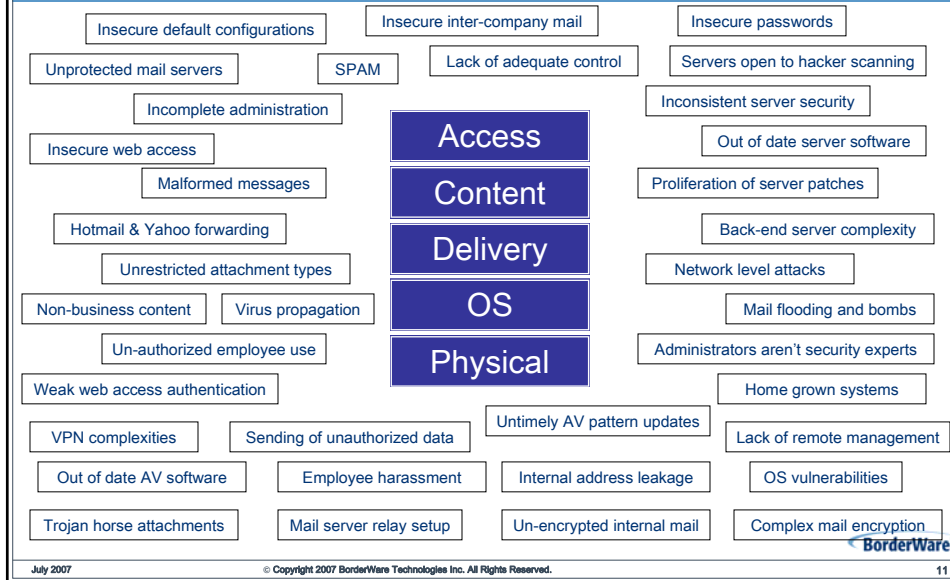
BorderWare

July 2007

© Copyright 2007 BorderWare Technologies Inc. All Rights Reserved.

10

The Threats - Email



The Threats – HTTP/FTP

- Viruses/Trojans/Worms
- Executables
- Peer to Peer
- Extortion
- Bandwidth
- Compliance/Corporate Governance/Legal Liability
- Outbound content
 - Blogs
 - Webmail content and attachment
 - Privacy
 - Corporate governance
 - Legal liability

The answer is not simply to block!

The Threats - IM

- SPAM
- Malicious attachments
- Directory harvesting
- Viruses/Trojans/Worms
- Extortion
- Compliancy/Corporate Governance/Legal Liability
- Bandwidth
- Outbound content
 - Body
 - Attachment
 - Privacy
 - Corporate governance
 - Legal liability

The answer is not simply to block!

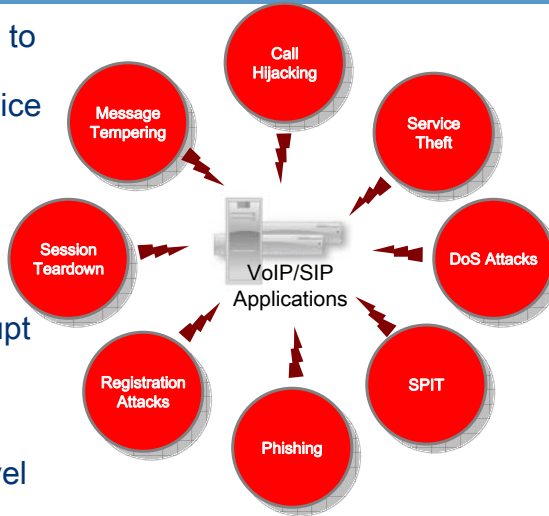
The Threats – VoIP

- Network level attacks
 - DoS Attacks
 - SYN floods
 - Ping attacks
- Protocol level attacks
 - Malformed message attacks
 - SIP DoS attacks
 - Buffer overflows
 - Bye attacks, Call Transfers, more
- Application level attacks
 - Service Theft
 - Eavesdropping
 - SPIT
 - Directory Harvesting
 - Many more

The answer is not simply to block!

Threats & Reliability - VoIP

- Users are accustomed to a high quality, highly reliable telephony service
- With VoIP, telephony systems are open to a whole range of new attacks
- Attacks need not be 100% effective to disrupt service
- Specialised security is required to ensure appropriate service level can be provided



July 2007

© Copyright 2007 BorderWare Technologies Inc. All Rights Reserved.

BorderWare

15

VoIP Threats and solutions

Rank	Risk	Solution
1 ★	Quality and Reliability, real or perceived ("as good as Skype" doesn't cut it)	New Telco services Network Quality of Service (QoS) controls
2 ★	Service Degradation/Disruption	QoS and Denial of Service controls
3 ★	Call Disruption	VoIP Application Security
4 ★	Call Spoofing	VoIP Application Security
5 ★★	Call Flooding/Spam	VoIP Application Security
6 ★	IP Network level attacks	Firewall Security Controls
7 ★★	Eavesdropping/Call Monitoring	Encryption Services
8 ★	Compliance issues	Content Controls and Policy
9 ★	Management Challenges	Managed Security

Security Categories: ★ Application, ★★ Converged, ★ Firewall

BorderWare

July 2007

© Copyright 2007 BorderWare Technologies Inc. All Rights Reserved.

16

VoIP Security – Risks and Consequences

Rank	Risk	Consequences
1	Quality and Reliability, real or perceived ("as good as Skype" doesn't cut it)	Degraded quality, end-user resistance to service acceptance
2	Service Degradation/Disruption	Degraded quality, total Service failure
3	Call Disruption	Partial service failure, end-user dissatisfaction
4	Call Spoofing	Phishing, legal liability
5	Call Flooding/Spam	End-user dissatisfaction
6	IP Network level attacks	Degraded quality, total Service failure
7	Eavesdropping/Call Monitoring	Confidentiality issues
8	Compliance issues	Entry barriers, implementation complexity
9	Management Challenges	Entry barriers, complexity

BorderWare

July 2007

© Copyright 2007 BorderWare Technologies Inc. All Rights Reserved.

17

Trends driving Communications Convergence

Complexity of Threat

- More types of communications
- Increasing sophistication of threats

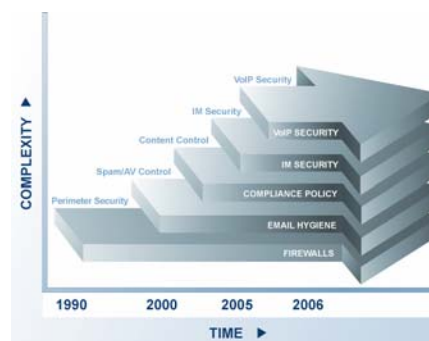
Content

- Shift from packet to content
- Not just inbound, now outbound content

Costs of Ownership

- Cost of acquisition
- Complexity and cost of operations
- Compliance Costs

Diverse Threat Landscape



\$4 Billion Market by 2010

BorderWare

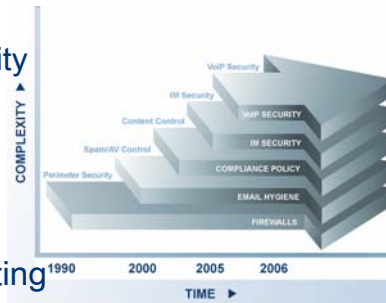
July 2007

© Copyright 2007 BorderWare Technologies Inc. All Rights Reserved.

18

Communications Convergence – The Problem

- Already have Firewall/Email security solutions
 - Yet NO security for IM, VoIP/SIP
 - Only URL blocking for web filtering
- Blended attacks are increasing
- Administrators spend hours creating policies, administering systems, generating reports and quarantine
- Disparate point products to solve the problem – doubling or tripling efforts
- Compliance needs to protect more than just email...



BorderWare

July 2007

© Copyright 2007 BorderWare Technologies Inc. All Rights Reserved.

19

What the Analysts are Saying

"Organizations are increasingly buying messaging security solutions that **address multiple threats** and deliver **integrated antivirus, anti-spam, and content filtering** in a **single solution**. Security appliances are quickly becoming the platform of choice for integrating multiple messaging security technologies." *IDC – March 2006 - Worldwide Secure Content Management 2006-2010 Forecast*

"As communications channels become more diverse, an effective content inspection **policy needs to span not only e-mail but also Web mail, IM, blog postings, chat rooms** and so on if it is to be comprehensive. Moreover, having separate policy and policy definitions, groups and directories is nonsensical...A single policy engine that can define communications policy across all modes of communications for groups and users is necessary..." *Gartner 2006*

"**Content inspection, compliance, and retention policies must cut across all communications media** rather than be silos in themselves. Organizations do not want to create a new Health Insurance Portability and Accountability Act (HIPAA) or ethical-wall policy for each communication medium." *Gartner 2006*

"The **key to scalability** is to provide a **component architecture** for enforcement but **with a single management layer to apply policy**" *Gartner 2006*

BorderWare

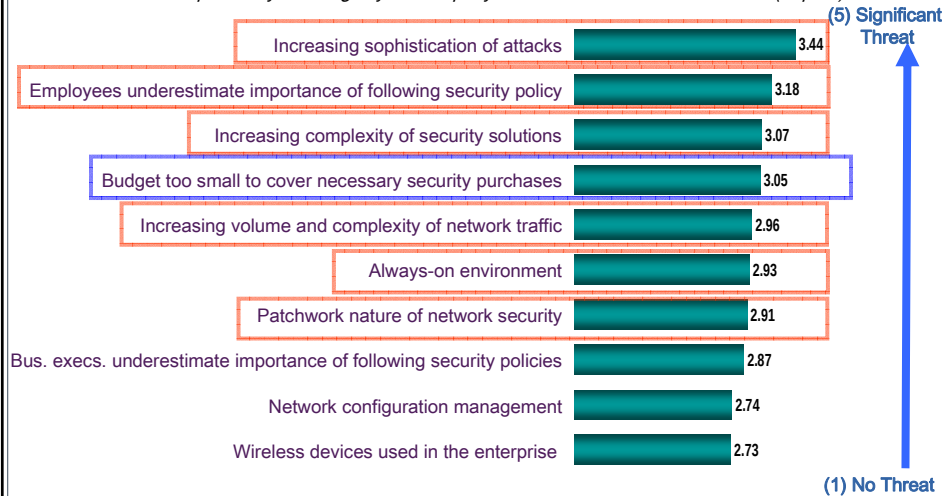
July 2007

© Copyright 2007 BorderWare Technologies Inc. All Rights Reserved.

20

IDC - Future Security Challenges

Q: Please rate the top security challenges your company will face over the next 12 months (Top 10)



Source: IDC's Enterprise Security Survey

July 2007

© Copyright 2007 BorderWare Technologies Inc. All Rights Reserved.

BorderWare

21

It's Not Just Email Anymore....

It's about securing all messaging applications....

- Email continues to be mission critical...300M in 2000; 800M in 2006
- Web Mail on the rise...150M in 2000; 850M in 2006
- Instant Messaging...175M+ business users in 2006
- Blogs and Wikis...0 to 50M in 3 years
- VoIP uptake increasing, taken to the network edge to reap benefits...

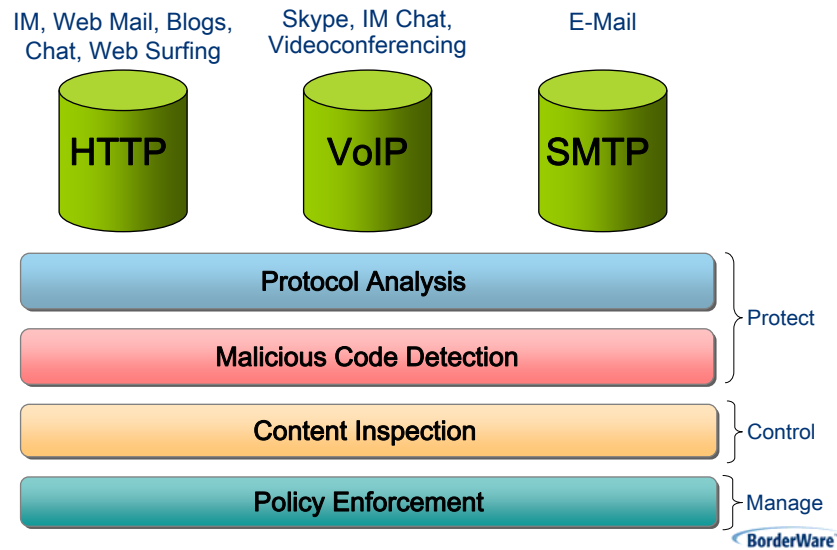
BorderWare

July 2007

© Copyright 2007 BorderWare Technologies Inc. All Rights Reserved.

22

Gartner's Message to Clients "Create Integration Points"

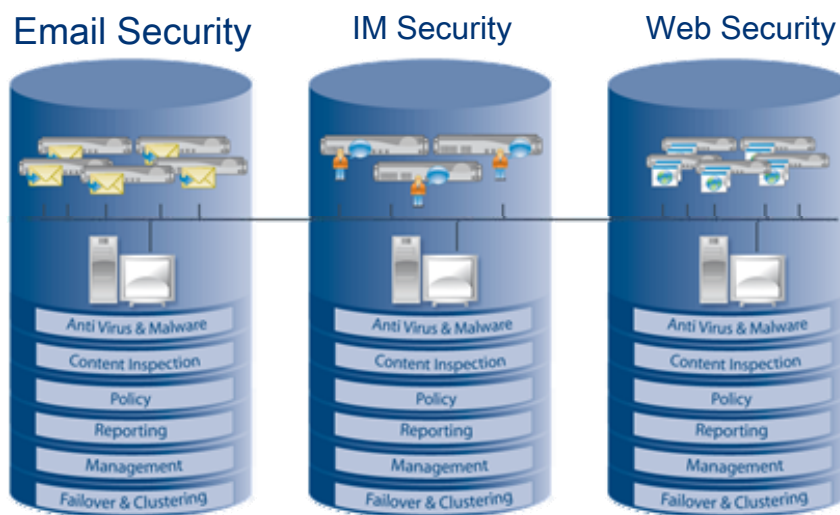


July 2007

© Copyright 2007 BorderWare Technologies Inc. All Rights Reserved.

23

Point Solutions, Today's - Perimeter Security Infrastructure



July 2007

© Copyright 2007 BorderWare Technologies Inc. All Rights Reserved.

24

Customer's Security Infrastructure...Fragmented

- Messaging security products exist as "Silos" creating gaps in policy and enforcement
- Threat experience is not leveraged across email, IM, web
- Silos increasingly consume IT capital and operational budgets
- High degree of employee expertise is required
- Scalability, availability, and redundancy are inefficient and expensive
- Lack of consolidated reporting drives inconsistent policy enforcement leading to financial risk

Summary:
Integration and consolidation enhances security and lowers TCO

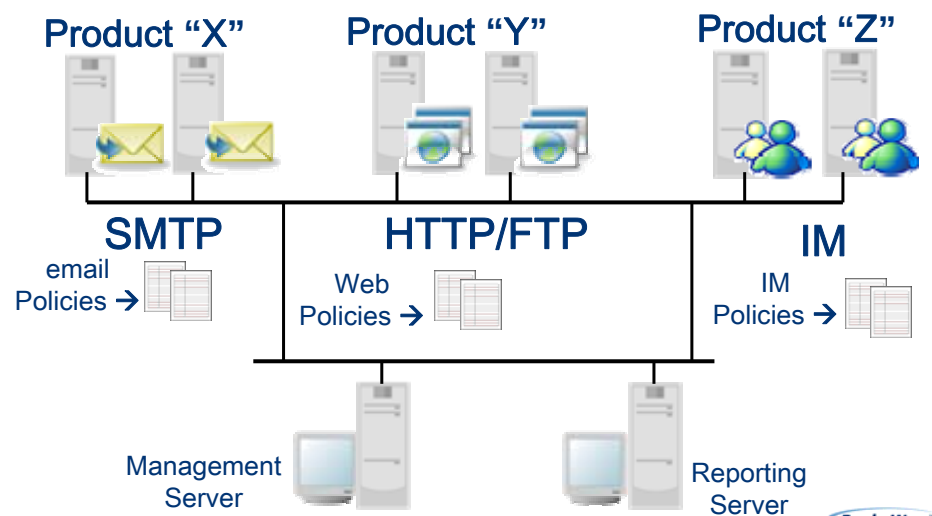
BorderWare

July 2007

© Copyright 2007 BorderWare Technologies Inc. All Rights Reserved.

25

Solving the problem - Organizations Today



July 2007

© Copyright 2007 BorderWare Technologies Inc. All Rights Reserved.

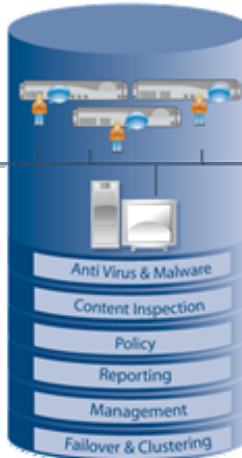
26

Point Solutions, Today's - Perimeter Security Infrastructure

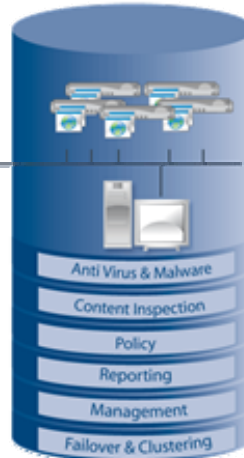
Email Security Silo



IM Security Silo



Web Security Silo



BorderWare

July 2007

© Copyright 2007 BorderWare Technologies Inc. All Rights Reserved.

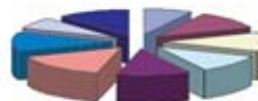
27

Point solutions – not the answer

Partial solution



Complete solution



- Spam Controls
- Content Filtering
- Virus Scanning
- Attachment Control
- Email Encryption
- Secure WebMail
- Policy Control
- Clustering
- User Based Spam Facilities

- Dedicated hardware required
- Dedicated operating system required
- Patch management and upgrades
- Cannot be deployed at gateway (W2K)
- Costly, management, overhead etc
- No integration, weighting, scoring
- No centralized management
- No centralized policy & reporting

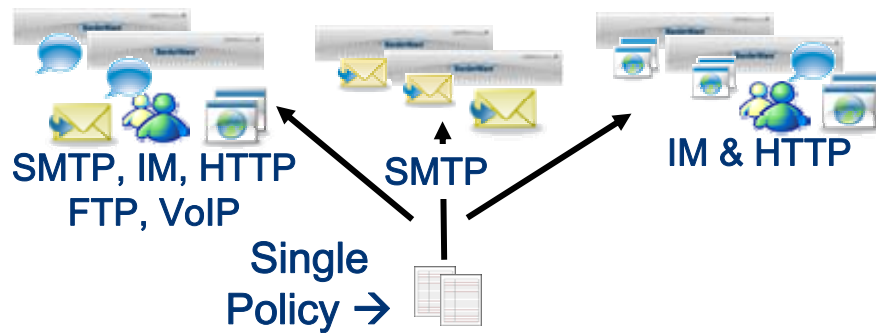
BorderWare

July 2007

© Copyright 2007 BorderWare Technologies Inc. All Rights Reserved.

28

The Converged Security Platform approach



- Single policy for all messaging protocols
- No additional management console or reporting server needed...
- Cluster of two or more appliances...

BorderWare

July 2007

© Copyright 2007 BorderWare Technologies Inc. All Rights Reserved.

29

Introducing, The BorderWare Security Platform

Elevator Pitch

- **What is it...**
"Consolidated Messaging Security Platform delivering integrated protection, control, and management for email, web, IM and VoIP"
- **Customer - Core Value Proposition**
"Enhanced Messaging security that's simple to use, with high performance, and low TCO"
- **What concerns does it address**
 - Inbound/Outbound Security & Content Risk
 - Complexity or disparate systems
 - Costs of products, management, renewals etc...

BorderWare

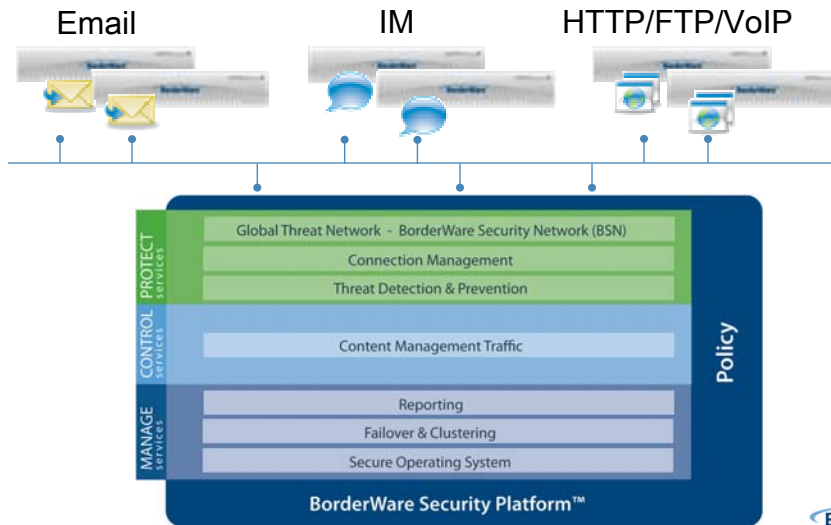
July 2007

© Copyright 2007 BorderWare Technologies Inc. All Rights Reserved.

30

Underlying Platform Architecture

Protect - Control - Manage



July 2007

© Copyright 2007 BorderWare Technologies Inc. All Rights Reserved.

31

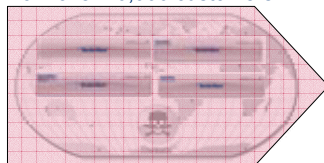
BorderWare Security Platform

BorderWare Security Network

Connection Management

- Real-time, multi-application reputation service
- Half billion sources of content layer threat information gathered from email, IM, Web, VoIP from over 10,000 customers
- Proactive defense to block unwanted and malicious content at network edge
- Reputation scoring for Web, email, IM, and VoIP
- Seamless integration with BorderWare Security Platform providing correlated reputation score across email, web, IM, VoIP
- Pinpoint accuracy with Domain and user reputations...

Over Half Billion Sources
From over 10,000 customers



Good
Reject



to over 10,000
customers worldwide

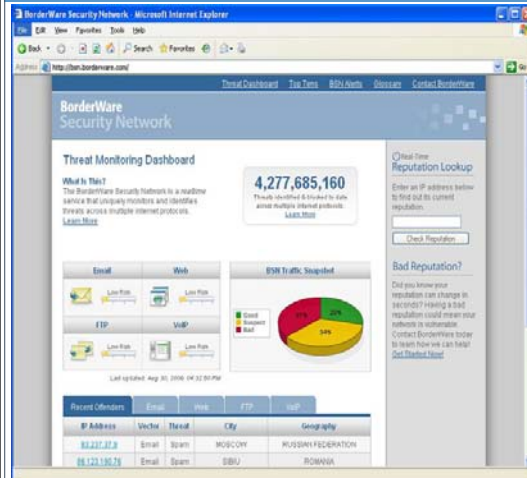
July 2007

© Copyright 2007 BorderWare Technologies Inc. All Rights Reserved.

32

Borderware Security Network - BSN

IP Reputation and Behavior Analysis



<http://bsn.borderware.com>

- Real time service that gives every device access to the address of known or suspected threats
- Covers, VoIP, Email, Web and other applications
- Provides proactive protection through real-time behavior analysis
- Cross references and analyses threat data across multiple protocols

BorderWare

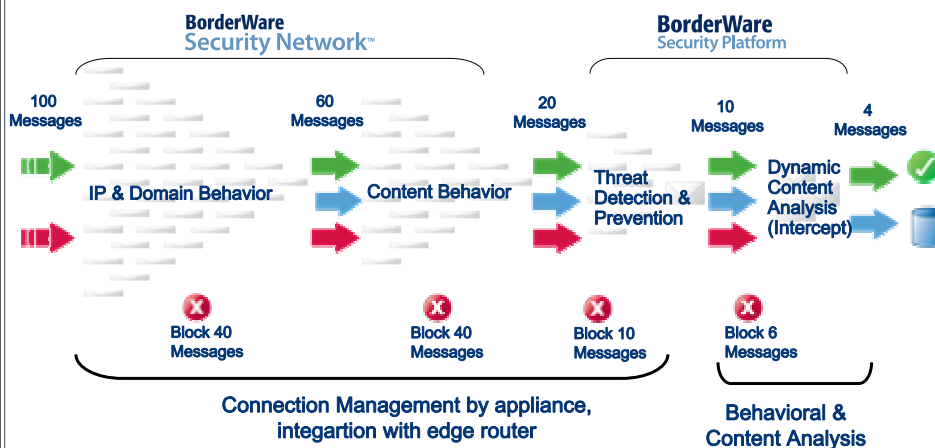
July 2007

© Copyright 2007 BorderWare Technologies Inc. All Rights Reserved.

33

BorderWare Security Platform

Edge Threat Protection



BorderWare

July 2007

© Copyright 2007 BorderWare Technologies Inc. All Rights Reserved.

34

BorderWare Security Platform

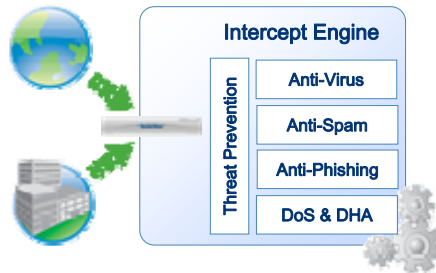
Real time, proactive threat protection

IP Reputation and Behavior Analysis

Intercept Security Engine

Multi-layered threat mitigation

- Reputation Checking
- Anti-Virus Scanning
- Threat Outbreak Protection
- File Attachment Analysis
- Anti-Spam
- Anti-Phishing



- Zero Hour Virus Protection
- Malware Protection
- Zombie PCs/Botnet Protection

Proactive, real-time, multi-layered threat prevention to block ALL email borne threats – not just spam!

BorderWare

July 2007

© Copyright 2007 BorderWare Technologies Inc. All Rights Reserved.

35

BorderWare Security Platform

Powerful content inspection

Control Content

- Policy Driven filter rules
 - User, group and domain based policies
 - Policy driven protocol independent content filtering
- Deep content inspection including
 - Ability to scan both in coming and outgoing messages – Email, IM, Web
 - Attachment control
- Compliance dictionaries
 - Multiple dictionary (OCF) support with pre-defined dictionaries for porn, vulgar, spam, content control and compliance
 - HIPAA, GLBA, SOX
 - User configurable/customizable
 - Weighted for accuracy

BorderWare

July 2007

© Copyright 2007 BorderWare Technologies Inc. All Rights Reserved.

36

BorderWare Security Platform

Simple to use Policy Management

Manage Infrastructure

Policy Editor

- Designed to simplify use and increase usability within minutes of deployment
- Reduce administration overhead
 - > Configure and manage all cross-protocol rules (Email, IM and Web)
 - > Consolidates a broad set of hygiene and content security capabilities into a single interface
- Administrators can implement:
 - > Domain, Group, and User policies
 - > Corporate, privacy, and compliance policies



July 2007

© Copyright 2007 BorderWare Technologies Inc. All Rights Reserved.

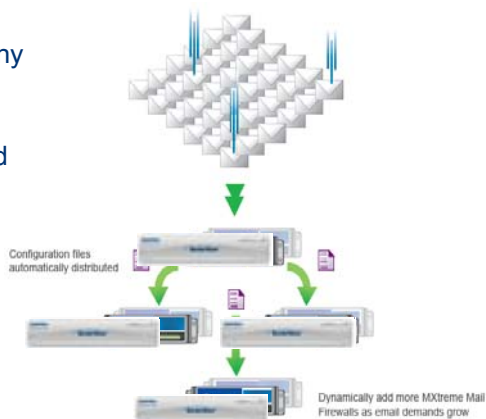
37

BorderWare Security Platform

Advanced \"On-Demand\" Clustering

Manage Infrastructure

- One-system set-up that can automatically replicate configurations
 - All members of cluster can run any application specific gateway service (email, IM, web)
 - All members leverage centralized policy for provisioning and management
 - On-demand scalability and load tuning
 - Eliminate single point of failure
- Quickly add systems with dynamic, on-demand clustering – removing a single point of failure, reducing administration and providing infinite scalability



July 2007

© Copyright 2007 BorderWare Technologies Inc. All Rights Reserved.

38

BorderWare Security Platform

Advantages - Summary

Capabilities		Benefits
360° security protection, control and management	➡	Enhanced Security
Integrated by design	➡	Reduced complexity
Modular in deployment	➡	Investment protection
Scalable architecture	➡	Investment leverage
Fault tolerant	➡	Proven Availability
Consolidated services, appliance delivery, easy management	➡	Low TCO
Built on a decade's worth of security software experience – 13 year security track record	➡	Peace of mind

Enhanced messaging security made simple, scalable, and affordable



July 2007

© Copyright 2007 BorderWare Technologies Inc. All Rights Reserved.

39

BorderWare Security Platform

Competitive Positioning

- BorderWare has a VERY unique position with BSP
- Traditional email competitors – Ironport, Secure Computing, Proofpoint, Barracuda
 - Point solutions for Web and IM
 - IM filter tied to HTTP protocol
 - Separate management appliance
 - No application level redundancy within cluster – email box can't run the web/IM proxy
 - No outbound web filtering – focused on inbound protection for AV, Phishing
- UTM Vendors – Fortinet/Watchguard
 - Focused on multi-protocol for inbound threats only
 - Limited Anti SPAM functions on inbound
 - No outbound content control; weighted dictionaries; email encryption
 - Separate management appliance
 - No Application level redundancy – special purpose boxes



July 2007

© Copyright 2007 BorderWare Technologies Inc. All Rights Reserved.

40

BorderWare Security Platform

Competitive Positioning

- Web Security Vendors – Websense; WebRoot; BlueCoat
 - URL Filtering – Websense, Webroot, BlueCoat
 - > Focus on URL filtering, data in motion and data at rest for web content
 - > No outbound content analysis – BlueCoat & WebRoot
 - > No Threat prevention on inbound or AV
 - > Limited to no email functions
 - > Limited IM filtering to HTTP protocol
 - > No centralized management for multi applications
 - > Limited scalability
 - Content Management – Content Management – Vontue, Tablus, Vericept
 - > Fingerprint data in motion and data at rest across network
 - > Indexed at client and server level
 - > Monitor all protocols for reporting and real time blocking - outbound
 - > No inbound threat management today – moving in this direction
 - > Hard to deploy – complex
 - > Not highly scalable



July 2007

© Copyright 2007 BorderWare Technologies Inc. All Rights Reserved.

41

Resources

- Independent white papers on:
 - HTTP threats
 - IM threats
 - VoIP threats
 - SMTP threats
 - Converged threats
- Independent verification, EAL, DSD, & ICASA
- Security track record – 14 years www.securityfocus.com
- Gartner, IDC, IDG, Forrester, Aberdeen Group

Contact – dean@borderware.com



July 2007

© Copyright 2007 BorderWare Technologies Inc. All Rights Reserved.

42

Conclusion – key takeaways

- Converged threats are already here, a solution is required now
- Threats are not limited to one protocol only
- Threats are not limited to inbound traffic only
- Disparate products are not the answer
- UTM's are not the answer
- Threats should be prevented at the gateway
- All gateway products should be deployed on a hardened and secure O/S with a proven track record
- Customers should look beyond the 'name' and adopt a multi vendor strategy

BorderWare addresses all of these threats...



July 2007

© Copyright 2007 BorderWare Technologies Inc. All Rights Reserved.

43



Q&A



dean@borderware.com